

2025年12月18日

報道関係各位

伊藤忠テクノソリューションズ株式会社

CrowdStrike Falcon Next-Gen SIEM を活用した
「CTC-SOC マネージドセキュリティサービス」を提供開始
AI を活用した脅威検知と対応を行う 24 時間 365 日のマネージドセキュリティ運用を実現

伊藤忠テクノソリューションズ株式会社(代表取締役社長:新宮 達史、本社:東京都港区、略称:CTC)は、クラウドストライクとのパートナーシップを拡大し、お客様システムを 24 時間 365 日リアルタイムで監視するセキュリティ監視・運用支援サービス「CTC-SOC^{※1}」に、CrowdStrike Falcon[®] Next-Gen SIEM を連携した新サービスの提供を開始しました。専任のセキュリティアナリストによる 24 時間 365 日の監視と AI による自動化で運用効率の向上を実現します。これにより、お客様の運用負担を軽減し、高度なセキュリティ監視・運用を提供します。

サイバー攻撃の高度化および AI を活用した攻撃の増加に伴い、企業では多様なセキュリティ製品の導入が進んでいますが、製品やシステム環境の違いによりログ管理が複雑化し、従来の SIEM^{※2} では分散したログの統合が難しい課題があります。さらに、収集したログを常時監視に活用するには、高度なセキュリティの専門知識が必要で、自社で 24 時間 365 日の監視体制を整えるのは容易ではありません。

こうした課題に対応するため、CTC-SOC マネージドセキュリティサービスは、専任のセキュリティアナリストによる監視体制と Falcon Next-Gen SIEM を組み合わせることで、持続的なセキュリティ監視と迅速な脅威の検知・対応を実現します。Falcon Next-Gen SIEM は、Falcon プラットフォーム上で多様なログをリアルタイムに収集・統合します。収集した Falcon プラットフォームのネイティブデータとサードパーティデータに加え、リアルタイムの脅威インテリジェンスと AI による自動化を組み合わせることで、単一ログでは見逃されやすい脅威を早期に検知します。これにより、SOC 運用に必要な脅威の可視化と高精度なアラートに加え、機械レベルの高速な対応を実現し、高度化する脅威や増大する監視データに適切に対応できます。

CTC はクラウドストライク認定の MSSP^{※3} として、Falcon Next-Gen SIEM を含むクラウドストライク社のライセンス管理や環境構築をエンドツーエンドで支援し、導入から運用までシームレスなマネージドセキュリティサービスを提供します。

今後も CTC は、長年培ってきたセキュリティの知見を活かし、進化するサイバー脅威や多様化するお客様のニーズに柔軟に対応しながら、信頼性の高いセキュリティサービスを提供します。

■ Falcon Next-Gen SIEM の主な機能

● セキュリティ運用の高速化

迅速な脅威の検知、インシデント調査の高速化、運用効率の向上を実現。サイバーセキュリティ人材の不足を補いながら、AI のスピードでより高度なセキュリティを実現。

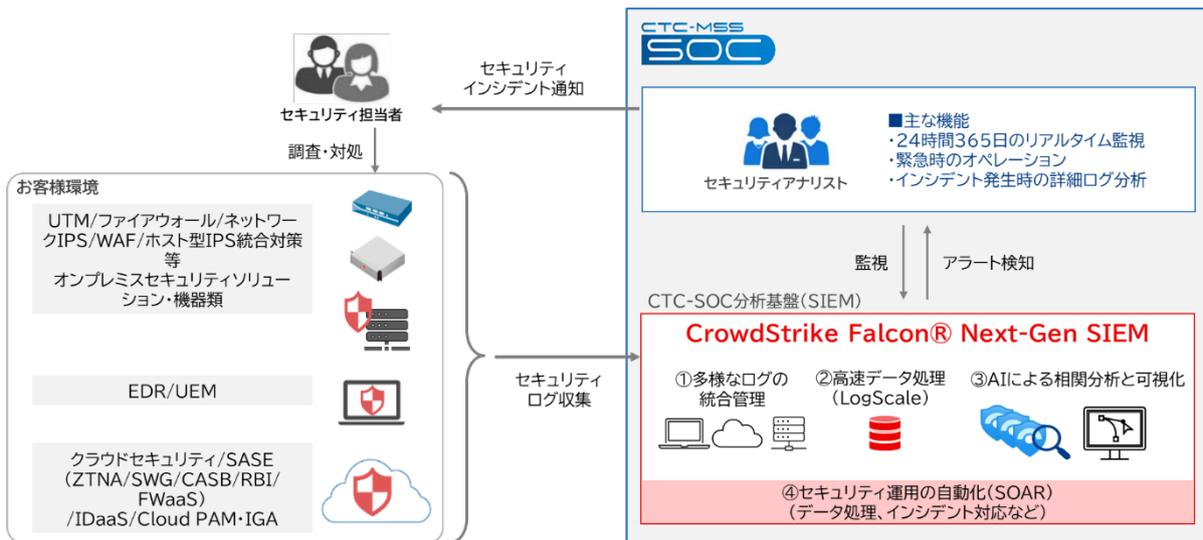
● 高速検索とリアルタイムでの共同作業

従来型の SIEM と比較して、最大 150 倍の検索速度を実現し、ペタバイト規模のログ容量にも対応が可能^{※4}。

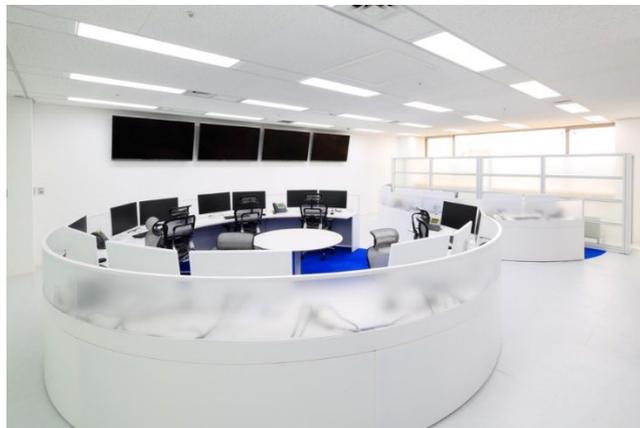
● 統合された可視性と対応

Falcon プラットフォームのネイティブデータとサードパーティのログを統合し、AI を活用した自動化とリアルタイムの脅威インテリジェンスを組み合わせることで、企業全体の可視性を高め、迅速かつ適切な対応を支援。

■ CTC-SOC と「CrowdStrike Falcon® Next-Gen SIEM」を組み合わせたサービスイメージ



■ CTC-SOC の運用環境



- ※1 CTC-SOC:CTC が 2014 年に日本国内で開設した、高度なセキュリティ監視サービスを提供するセキュリティ・オペレーション・センター(SOC)。2024 年にグローバル拠点となる「CTC Global SOC」をマレーシアに開設しました。最新の脅威情報と生成 AI を組み合わせた監視対応と複数のオプションを用意し、お客様の環境に合わせた最適な構成をご提案します。詳細は[こちら](#)。
- ※2 SIEM(Security Information and Event Management):セキュリティ情報およびイベントを管理・分析するシステム。
- ※3 MSSP(Managed Security Service Provider):企業や組織に代わって、セキュリティの監視や運用を専門的に行うサービス提供者。CTC は 2025 年 6 月にクラウドストライク社に MSSP として認定されました。
- ※4 本資料に記載されている結果は導入事例に基づくものであり、効果は環境により異なる場合があります。
- ※ その他、記載されている商品名などの固有名詞は、各社の商標または登録商標です。
- ※ 掲載されている情報は、発表日現在の情報です。最新の情報と異なる場合がありますのでご了承ください。

以上

<報道機関からのお問い合わせ先>
伊藤忠テクノソリューションズ株式会社
広報部
E-mail:press@ctc-g.co.jp